Détection de pairs suspects dans le réseau pair à pair KAD

Thibault Cholez, Christopher Hénard, Isabelle Chrisment, Olivier Festor, Guillaume Doyen, Rida Khatoun

Détection de pairs suspects dans le réseau pair à pair KAD

Thibault Cholez, Christopher Hénard*, Isabelle Chrisment*, Olivier Festor**, Guillaume Doyen, Rida Khatoun
Université de Technologie de Troyes, STMR (UMR CNRS 6279), France
*LORIA - ESIAL, Nancy University, France
**INRIA Nancy-Grand Est, France
Email : {firstname.name}@utt.fr ; {firstname.name}@loria.fr

***Résumé*—Les réseaux pair à pair (P2P), notamment ceux utilisant les tables de hachage distribuées, sont aujourd'hui des systèmes d'information majeurs comptant des dizaines de millions d'utilisateurs. Ils présentent cependant des vulnérabilités permettant l'insertion ciblée de nœuds pouvant réaliser plusieurs actions malveillantes (pollution, surveillance, déni de service). Nous présentons ici une étude visant à détecter les nœuds suspects dans un réseau P2P largement déployé à savoir KAD. Nous avons conçu pour cela un explorateur, dont nous détaillons la procédure et évaluons l'efficacité, permettant d'obtenir une vue précise du réseau. L'analyse des données collectées au travers de la répartition des identifiants pairs ainsi que de la distance entre les pairs et certains contenus nous a permis de mettre en évidence qu'au moins 2200 ressources du réseau sont attaquées durant nos observations.**

***Index Terms*—réseaux P2P, supervision, sécurité, indexation des contenus, attaque Sybil, détection d'attaque.**

I. Introduction

Les réseaux pair à pair (P2P) sont devenus une application majeure de l'internet en permettant à leurs utilisateurs de partager rapidement et sans coût d'infrastructure de grandes quantités de données. Parmi les différentes architectures pair à pair complètement distribuées, les tables de hachage distribuées (DHT) ont prouvé aussi bien en théorie qu'en pratique leur capacité à constituer des systèmes d'information performants. Basés sur l'architecture Kademlia, les réseaux P2P tels que KAD ou la DHT de BitTorrent (Mainline DHT) regroupent ainsi des millions d'utilisateurs.

Si l'absence de composant central apporte au paradigme P2P ses principaux avantages (passage à l'échelle, robustesse, absence de coûts d'infrastructure), il constitue également une limite en rendant difficile l'application de règles de sécurité. En effet, les pairs étant parfaitement autonomes, certains pairs malveillants peuvent détourner le protocole à leurs propres fins, telles que : la surveillance des échanges [1] [2] [3], la pollution [4] [5] [3], la suppression d'information [1] ou encore le déni de service distribué [6] [1] [7]. Si plusieurs attaques pouvant affecter les tables de hachage distribuées sont d'ores et déjà connues (attaque Sybil, attaque ciblée) et ont été expérimentées ponctuellement, aucune étude à ce jour ne s'est intéressée à recenser de telles attaques en pratique.

Nous proposons dans ce papier de détecter les pairs suspects dans le réseau P2P KAD. Pour cela nous réalisons une cartographie du réseau grâce à un explorateur spécifiquement conçu pour obtenir une image très précise de la DHT. Nous analysons ensuite les résultats afin de détecter deux types de positionnements suspects selon qu'ils impliquent localement un groupe de pairs malveillants ou uniquement un seul pair. Nous constatons ainsi pour la première fois la réalité de certaines attaques publiées et pouvons estimer leur nombre au sein du réseau.

Cet article est organisé comme suit : la section II présente le contexte du réseau P2P KAD et les travaux relatifs à l'exploration et la sécurité de ce réseau. Nous présentons ensuite dans la section III notre explorateur permettant la découverte des pairs avec une grande précision. Les images ainsi obtenues du réseau sont analysées dans la section IV où deux approches sont utilisées pour détecter les pairs suspects. Enfin, la section V conclut et présente nos travaux futurs.

II. Contexte et travaux relatifs

A. Le réseau KAD

KAD est un réseau P2P structuré basé sur le protocole de routage Kademlia [8] et implanté par les clients libres eMule [1] et aMule [2] qui permettent le partage de fichiers entre utilisateurs. Rendu populaire au fil des fermetures des serveurs eDonkey, KAD est principalement utilisé en Europe et en Chine et compte environ 3 millions d'utilisateurs simultanés, ce qui en fait l'un des plus importants réseaux P2P déployés.

Dans KAD, chaque pair ainsi que chaque information indexée dans le réseau possède un identifiant "KADID" de 128 bits définissant sa place sur la DHT. Le routage est basé sur la métrique XOR grâce à laquelle on mesure la distance entre deux identifiants. La table de routage de chaque pair est organisée en un arbre dont les feuilles sont

1. http ://www.emule-project.net/
2. http ://www.amule.org/

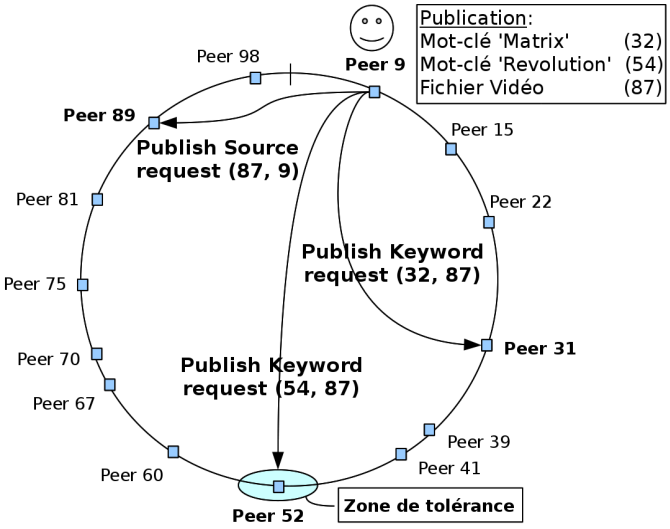

FIGURE 1. Indexation à deux niveau sur KAD

constituées de groupes de taille constante de K contacts ($K = 10$), la distance entre les contacts retenus et le pair courant étant divisée par deux (1 bit supplémentaire commun) à chaque niveau de l'arbre. Ainsi le niveau **i** représente une portion du réseau de taille $n/2^i$, donc d'autant plus petite que celle-ci est proche du pair courant. Cette organisation permet de localiser efficacement les identifiants recherchés en O(log n) messages, n étant la taille du réseau.

En tant que support au partage de fichiers, la fonction principale de la DHT de KAD est d'indexer des mots-clés et des fichiers selon la procédure présentée par la figure 1. Lorsqu'un fichier est partagé (dans l'exemple, le fichier vidéo nommé « matrix_revolution.avi »), son contenu ainsi que chaque mot-clé constituant le nom du fichier sont hachés par une fonction MD4 (donnant les identifiants 32, 54, 87 pour respectivement chacun des mots-clés et le fichier). Les identifiants ainsi générés sont ensuite publiés sur le réseau. Les pairs chargés de l'indexation d'une information sont les dix pairs dont les identifiants sont les plus proches de celui de l'information. L'assignation des identifiants des pairs n'est donc pas strictement contrainte, bien qu'utilisant normalement une fonction aléatoire, alors que les identifiants des mot-clés et fichiers indexés sont obtenus par la fonction de hachage MD4.

Un mécanisme de double indexation permet de retrouver un fichier correspondant à un ensemble de mots-clés. Pour publier un fichier, deux types de requêtes sont nécessaires :

- les requêtes `KADEMLIA2_PUBLISH_KEY_REQ` sont envoyées vers l'identifiant des mots-clés et associent un mot-clé (32 ou 54) avec un fichier (87) ;
- les requêtes `KADEMLIA2_PUBLISH_SOURCE_REQ` sont envoyées vers l'identifiant du fichier (87) et associent un fichier avec une source (le pair 9 le partageant).

La réalisation de services (publication ou recherche) se fait en deux étapes. Dans un premier temps, le processus de localisation trouve les pairs les plus proches de l'identifiant de l'information visée (en émettant des requêtes *KADEMLIA2_REQ* de manière itérative), puis les requêtes spécifiques au service demandé sont envoyées à ces pairs.

B. La sécurité des DHT

Plusieurs problèmes de sécurité ont été mis en évidence dans cette architecture. En expérimentant le principe de l'attaque Sybil [9] dans KAD, qui consiste à insérer de nombreux pairs factices contrôlés par une même entité, les auteurs de [1] ont montré que le réseau était très vulnérable et pouvait être largement affecté par une attaque émise d'une seule machine. En effet, après avoir découvert les pairs d'une zone de la DHT, les auteurs ont pu y injecter de nombreux Sybils ($2^{16} = 65535$ contre environ 10000 pairs légitimes) obtenant ainsi le contrôle de cette zone en y interceptant la grande majorité des messages. En restreignant la zone d'attaque au voisinage immédiat d'une information, il est également possible d'en prendre le contrôle avec moins de Sybils (une vingtaine). Le vecteur d'attaque utilisé ici est la table de routage des pairs, les Sybils s'annonçant directement pour se propager.

Dès lors, certains mécanismes de protection ont été implantés pour protéger la table de routage de telles attaques [10]. De nouvelles contraintes empêchent dorénavant deux pairs affichant une même adresse IP d'être insérés dans une même table de routage. De même, deux pairs appartenant au même sous-réseau ne peuvent pas être trop proches dans une même table de routage, c'est à dire dans la même feuille de l'arbre. Cependant, nous avons montré dans nos précédents travaux [3] que les attaques ciblées peuvent utiliser des nœuds distribués sur le réseau IP et continuer d'être efficaces avec peu de ressources. Le schéma 2 montre les échanges de messages nécessaires à la réalisation d'un service sur KAD lorsqu'une référence est attaquée. Les pairs malveillants sont ainsi insérés plus proches que n'importe quels autres de la ressource visée (96 bits en commun) et coopèrent pour attirer les requêtes de service.

Plusieurs applications exploitent cette vulnérabilité. Les nœuds ainsi insérés en des points spécifiques constituent autant de sondes capables de surveiller les messages échangés au sein du réseau P2P. [1] surveille ainsi une portion complète de la DHT, [3] s'intéresse à des mots-clés spécifiques et annonce des pots de miel alors que [2] place des sondes de manière à recevoir une copie du trafic émis vers chaque pair du réseau. Ces pratiques posent des problèmes de vie privée pour les utilisateurs du réseau.

D'autres attaques sont également possibles : les auteurs de [1] ont réalisé une attaque de type éclipse faisant disparaître de l'indexation du réseau le contenu ciblé. Ils ont aussi expérimenté, tout comme [6], un déni de service distribué en injectant systématiquement l'adresse IP d'une

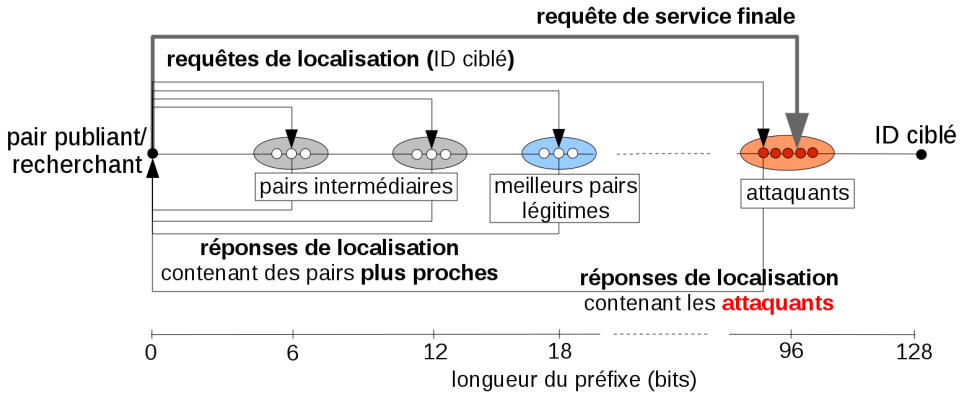

FIGURE 2. Prise de contrôle d'une référence sur la DHT de KAD

machine victime dans les réponses émises par les Sybils et générant ainsi plus de 100Mbit/sec de trafic. Les auteurs de [4] ont montré que la DHT d'Overnet pouvait être polluée efficacement par l'insertion de nœuds autour de certains mots-clés. Ce problème affecte également KAD [5]. Nous avons montré dans [3] que l'attaque locale permettait en outre de polluer efficacement le réseau en générant à faible coût de faux fichiers très attractifs ce qui peut amener les utilisateurs à télécharger des contenus indésirables et illégaux (virus, contenu pédophile, ...) à leur insu.

Bien que nous ayons proposé dans [11] une méthode capable de détecter les attaques ciblées analysant la distribution des identifiants autour d'une ressource sur la DHT, celle-ci n'est pas déployée à grande échelle, laissant le réseau vulnérable aux attaques sus-mentionnées.

C. L'exploration de DHT

Un explorateur ou "*crawler*" est un outil capable de découvrir l'ensemble des pairs d'un réseau et de stocker les différentes informations les concernant.

Plusieurs explorations du réseau KAD ont déjà été réalisées à diverses fins. Les auteurs de [7] et [1] découvrent ainsi les pairs du réseau à des fins d'attaque. Pour chaque pair découvert, ils interrogent ce dernier en émettant de nombreuses requêtes de localisation (*Kademlia request*) vers des identifiants pré-calculés de manière à obtenir tous les contacts de la table de routage du pair interrogé. Ces informations servent ensuite à insérer des Sybils [7] ou à corrompre les références de contacts existants [1]. Utilisant le même explorateur *Blizzard* que [7], [12] réalise des explorations périodiques de la DHT de manière à étudier certaines caractéristiques des pairs dans le temps.

Les auteurs de [13] utilisent une autre approche basée sur l'interrogation de contacts par des requêtes d'amorçage (bootstrap request). Cette approche est sensée être plus performante (20 contacts retournés par requête d'amorçage contre 11 pour celle de localisation). Cependant les contacts obtenus sont choisis aléatoirement dans la table alors que les requêtes de localisation spécifient une adresse cible permettant de contrôler le parcours des tables. Les résultats de cette exploration ont mis en évidence un nombre important de pairs (20%) partageant leur identifiant dont les auteurs étudient les causes possibles.

Si de nombreuses observations du réseau KAD ont été réalisées, aucune jusqu'à présent ne s'est intéressée à recenser les attaques pouvant affecter la DHT. De même, aucune n'estime l'efficacité de leur explorateur dont les algorithmes sont peu détaillés, s'ils sont mentionnés.

III. EXPLORATION DU RÉSEAU

A. Méthode d'exploration

La conception de notre explorateur vise deux objectifs. D'une part, obtenir une vision précise du réseau, et d'autre part, limiter l'empreinte de l'exploration sur le réseau en limitant le nombre de requêtes envoyées à chaque pair. Ceci permet en outre d'obtenir une exploration compatible avec les limitations implantées dans les derniers clients, contrairement aux précédentes stratégies d'exploration désormais limitées, notamment par rapport à la protection contre l'inondation empêchant un pair de recevoir rapidement des messages d'une même source.

Notre méthode d'exploration se divise en trois phases décrites ci-après.

Amorçage: La phase d'amorçage sert à obtenir une première image imprécise de l'ensemble de la DHT. Pour cela, des requêtes d'amorçage (bootstrap) sont émises. Les requêtes d'amorçage permettent d'obtenir 20 contacts tirés aléatoirement dans la table de routage du pair sollicité et sont donc parfaitement adaptées à une première découverte globale de la DHT. De nouveaux contacts sont ainsi progressivement interrogés au fur et à mesure des réponses jusqu'à ce que 500000 contacts aient été découverts dont au moins 500 par zone[3]. Au delà de cette valeur, les contacts retournés étant sélectionnés au hasard, il est de plus en plus difficile d'apprendre de nouveaux contacts par cette méthode.

3. une zone est une subdivision artificielle de l'espace d'adressage basée sur le premier octet de poids fort des identifiants (de *0x00* à *0xFF*)

Exploration complète: Ensuite, chaque zone est explorée avec précision grâce aux requêtes de localisation (kademlia request). Un pair ainsi interrogé retourne les 4 contacts les plus proches connus de l'identifiant spécifié en paramètre. Afin de découvrir l'ensemble des pairs, nous générons $2^{21} \approx 2$ millions de « KADIDs cibles » uniformément répartis et envoyons pour chacun d'eux une requête de localisation au pair le plus proche déjà découvert. Ainsi, $2^{13}(2^{21}/2^8)$ KADIDs cibles sont générés dans chaque zone selon le format :

$$\underbrace{ZZZZZZZZ}_{8\ bits\ de\ la\ zone}\overbrace{FFFFFFFFFFFFF}^{13\ bits\ fixés\ de\ 0\ à\ 2^{13}-1}\underbrace{RRRRRR...R}_{107\ bits\ aléatoires}$$

où Z, F et R désignent respectivement des bits de zone, les bits fixés et ceux tirés aléatoirement une fois.

Seconde passe: Dès qu'une zone a été explorée, c'est à dire quand tous les KADIDs cibles de cette zone ont été envoyés, une seconde exploration de celle-ci a lieu pour en améliorer la cartographie. Pour chaque contact précédemment découvert, on calcule alors son voisin le plus proche dont on extrait ensuite le préfixe commun de longueur x bits entre les deux KADIDs. On construit ensuite un nouveau « KADID cible » partageant ce préfixe et où les $(128 - x)$ bits restants sont aléatoires. Une requête de localisation pour ce KADID cible est finalement envoyée au contact. Cette phase permet de découvrir quelques contacts manqués lors de l'exploration complète. L'exploration se termine lorsque tous les contacts ont ainsi été interrogés sur leur voisinage immédiat.

B. Cartographie obtenue

Informations enregistrées: Pour chaque pair découvert, nous enregistrons les informations suivantes <KADID, adresse IP [4], port TCP, port UDP, version de KAD, état du pair>. La version de KAD fait référence à la version du protocole implantée par le client, l'état du pair est P(*possible*), T(*tried*) ou R(*responded*) selon respectivement que le contact a juste été découvert, a été contacté ou a répondu.

```
[...]
<32FFF76959F6A7095347FB338B304330,@IP,38060,16905,0,T>
<32FFFC5C4D5AE9A082871FF68B1F0D9C,@IP, 5149, 1025,4,R>
<32FFFC5C4D5AE9A082871FF68B1F0D9C,@IP, 5149, 5159,4,P>
Zone 33: 15196 contacts
<3300048A90460A8AAC3DD2FF542ADF98,@IP,12399,39949,9,R>
<3300083A0480CFA91B8C142401DD26F2,@IP, 5611, 5621,8,T>
<330018506569424D7CBA7133F437EDC8,@IP, 6647, 6657,8,P>
<33002596F7AAAA4348FB4349F0A14FA4,@IP,46318,61632,9,R>
<33002EF905E27753B1900BC602D29C20,@IP,19774,19774,8,T>
<33004546934FABE9685674DE1598548F,@IP,51478,52073,9,R>
[...]
```

Résultats généraux: L'exploration d'une zone compte entre 13000 et 17000 contacts, le nombre total de pairs mesuré allant de 3,3M à 4,3M selon le jour et l'heure de l'exploration. D'un point de vue macroscopique, la répartition des pairs sur l'ensemble de l'espace d'adressage de la DHT est bien uniforme (figure 3), conformément à ce qu'on peut attendre de la majorité des pairs légitimes générant aléatoirement leur identifiant à la première connexion.

Nous analysons plus précisément les résultats d'exploration dans la section suivante, avec pour objectif de détecter les placements traduisant des comportements déviants. Les résultats obtenus pour les différentes explorations réalisées étant similaires, la suite de cet article utilise les données d'une exploration réalisée le 8 Juillet 2010 et comptant 3688932 pairs.

C. Évaluation

Nous avons évalué notre explorateur de deux façons. Nous avons tout d'abord injecté 360 pairs dans KAD suivant une configuration d'attaque depuis l'infrastructure d'expérimentation distribuée PlanetLab [5]. Les Sybils sont ainsi répartis par groupe de 5 sur 72 identifiants cibles dont ils partagent au moins 96 bits. A l'issue d'une exploration du réseau concomitante à l'attaque, la totalité des pairs insérés étaient bien présents dans les résultats de l'exploration. L'extrait ci-dessous montre une analyse des données recherchant les pairs à proximité d'identifiants donnés en paramètre (ici les 72 identifiants ciblés).

```
[...]
KADID 71: 19856E29730F11CA0E0C210630ADCB36
<19856E29730F11CA0E0C210621142E70,62.108.171.74,
14337, 13602, 8, T> [prefix = 99]
<19856E29730F11CA0E0C2106546F8C89,193.167.187.186,
 14690, 13799, 8, T> [prefix = 97]
<19856E29730F11CA0E0C21065622F60F,155.245.47.241,
 13953, 13779, 8, T> [prefix = 97]
<19856E29730F11CA0E0C210676E74885,212.51.218.235,
 13897, 14465, 8, T> [prefix = 97]
<19856E29730F11CA0E0C21069636476A,129.97.74.14,
 14308, 13853, 8, T> [prefix = 96]
KADID 72: EBCBA6D72037ED01F56809A9FFE6A86E
<EBCBA6D72037ED01F56809A9268DA7FB,155.245.47.241,
 13915, 13842, 8, T> [prefix = 96]
<EBCBA6D72037ED01F56809A94519B1D4,129.97.74.14,
 14029, 13914, 8, T> [prefix = 96]
<EBCBA6D72037ED01F56809A9702F72B7,193.167.187.186,
 13666, 14427, 8, T> [prefix = 96]
<EBCBA6D72037ED01F56809A9892C91A4,62.108.171.74,
 13853, 14683, 8, T> [prefix = 97]
<EBCBA6D72037ED01F56809A9BAD2A19E,212.51.218.235,
 13861, 13939, 8, R> [prefix = 97]

72/72 of the proposed KADIDs are targeted with
at least 96 bits by:
37 IP addresses (representing 361 different KADID)
21 subnets /24  (representing 362 different KADID)
```

Une seconde évaluation a consisté à modifier un client KAD afin d'afficher la liste des contacts trouvés lors d'une publication et à explorer conjointement la zone correspondante. L'ensemble des pairs trouvés par le client aMule l'a

4. certaines adresses IP sont anonymisées dans le cadre de cet article

5. http ://www.planet-lab.org/

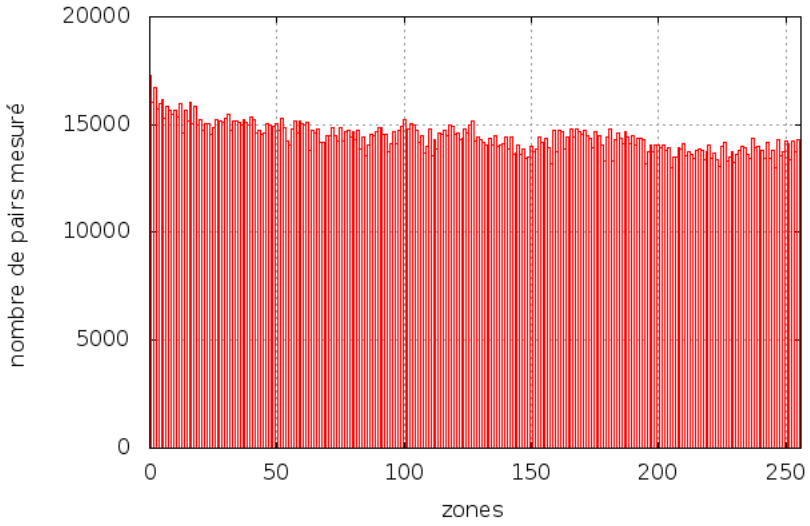

FIGURE 3. Répartition des pairs sur la DHT

également été par l'explorateur, ce qui tend également à montrer l'efficacité de notre exploration.

IV. Détection des pairs suspects

Comme expliqué précédemment, une attaque sur la DHT implique l'insertion d'un ou plusieurs pairs à proximité de l'identifiant ciblé, afin d'attirer tout ou partie des requêtes à son attention. Pour une meilleure efficacité, plusieurs pairs peuvent être insérés conjointement afin d'attirer davantage de requêtes.

A. Détection par densité des pairs

Notre première analyse s'intéresse à localiser de tels groupes de pairs sur la DHT. Nous cherchons ainsi à détecter les couples de pairs dont la distance trop proche traduit un placement intentionnel à proximité d'un tierce identifiant plutôt qu'un choix aléatoire de leurs identifiants.

$$F(x) = \frac{N}{2^x} \tag{1}$$

Soit F la fonction donnant le nombre moyen de pairs partageant x bits avec un pair courant étant donné un nombre total N de pairs dans le réseau. Nous considérons un nombre de 4 millions de pairs connectés simultanément. Le tableau I en présente certaines valeurs pour $N = 4 \times 10^6$ et $x \in [1; 128]$. De plus, le préfixe moyen partagé entre deux pairs consécutifs est de $d_{moy} = log2(N) = 21.93$ bits.

Étant donné notre exploration de la DHT, nous avons calculé le préfixe commun entre chaque pair et son plus proche voisin, les résultats sont présentés par la figure 4. Si les préfixes jusqu'à 35 bits sont communément partagés

Nombre de bits en commun	Nombre moyen de pairs
1	2,000,000
8	15625
12	976.5
16	61
18	15,25
20	3.8
24	0.24
28	0.015
32	$9.32 * 10^{-4}$
64	$2.17 * 10^{-13}$
96	$5.05 * 10^{-23}$
128	$1.17 * 10^{-32}$

TABLE I
NOMBRE MOYEN DE PAIRS PARTAGEANT UN PRÉFIXE AVEC UN IDENTIFIANT DONNÉ POUR UNE DHT DE 4 MILLIONS

entre voisins et ne permettent pas de détecter les attaques, les contacts partageant davantage de bits traduisent un placement intentionnel. Le premier graphe de la figure 5 illustre cette déviation de la norme théorique (équation 1) pour les contacts partageant entre 22 et 45 bits. Plus le préfixe commun est élevé, plus l'espérance de trouver de tels voisins est faible et traduit un placement intentionnel ce qui est illustré par le second graphe de la figure 5. Nous avons ainsi relevé 426 groupes de contacts anormalement proches (partageant un préfixe entre 35 et 127 bits) et traduisant autant d'attaques groupées potentielles. Cependant, l'écart le plus important concerne le préfixe de 128 bits (1 million de pairs) qui correspond aux pairs partageant exactement le même identifiant et mérite une analyse à part.

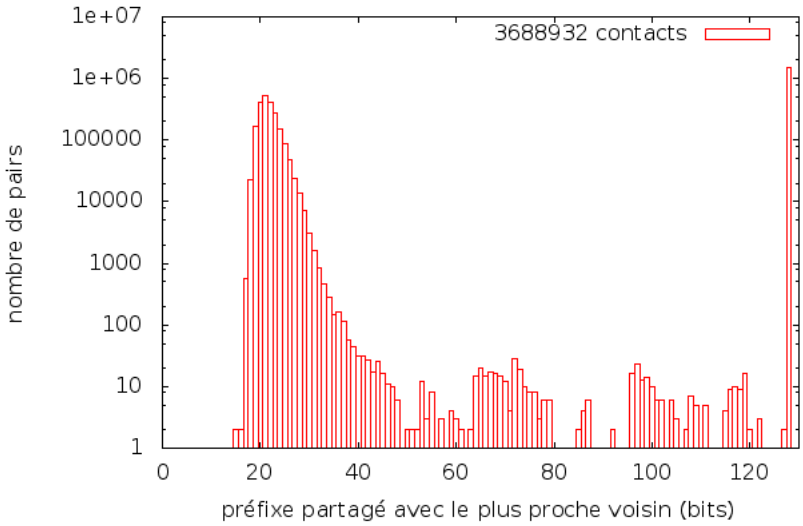

FIGURE 4. Répartition des préfixes entre voisins sur la DHT

Identifiants partagés: En effet, sur les 3688932 pairs trouvés lors de l'exploration, on ne dénombre après analyse que 2613963 KADIDs différents. Tout comme [13], nous constatons donc l'existence de KADIDs partagés par plusieurs pairs. Plus précisément, parmi les KADIDs relevés :

- 82,36% (2152900) des KADIDs sont utilisés par un pair unique,
- 17.64% (461063) des KADIDs sont partagés par plusieurs pairs dont :
  - 10,42% des KADIDs sont communs à 2 pairs,
  - 2,85% des KADIDs sont communs à 3 pairs,
  - les pourcentages décroissants jusqu'à 1 KADID partagé par 259 pairs.

Le partage de préfixe peut traduire une attaque si plusieurs pairs sont insérés exactement avec l'identifiant de la cible. Cependant, il peut également traduire un changement bénin de configuration d'un pair. En effet, un pair changeant d'adresse IP (allocation dynamique d'adresse, mobilité), ou de port de communication durant sa connexion au réseau apparaîtra deux fois avec le même identifiant le temps que la DHT mette à jour ses références. Afin d'éviter de compter ces cas, nous supprimons de la liste des identifiants suspects les cas pour lesquels deux pairs partagent un identifiant où seule l'adresse IP ou seul le port diffèrent entre les deux pairs. Ainsi parmi les KADIDs partagés entre deux pairs (272149) :

- 49.73% ne diffèrent que par l'adresse IP (ports UDP et TCP identiques),
- 26.91% ne diffèrent que par le port UDP,
- 1.44% ne diffèrent que par le port TCP,
- 21.92% sont suspects.

Par cette méthode, 248569 identifiants différents peuvent être suspectés. Malgré les précautions prises, ce chiffre peut être soumis à des faux positifs. De plus, les effets du partage d'identifiants entre pairs sur le réseau sont limités par des contraintes [10] locales appliquées par chaque client pour protéger sa table de routage lors de l'insertion d'un pair, ou protéger un service lors de la sélection des pairs découverts à l'issue d'une procédure de localisation. Notamment, seul un pair par KADID est autorisé et les autres sont ignorés. Nous proposons une dernière estimation plus fiable des attaques affectant KAD, car basée sur les contenus et non uniquement sur les pairs.

B. Détection par proximité aux ressources

Les analyses précédentes ont une limite importante : elles permettent d'identifier des attributions d'identifiants suspects sans pour autant pouvoir les corréler à un contenu précis. Par ailleurs, les analyses précédentes étant basées sur des proximités entre pairs, au moins deux pairs doivent être insérés pour être détectés, les attaques n'impliquant qu'un pair ne peuvent être détectées an analysant la densité des pairs.

Une manière fiable de détecter les attaques est donc de pouvoir mettre en évidence la proximité anormale des pairs malveillants par rapport à une ressource plutôt que la proximité des pairs entre eux. La difficulté de cette approche est que les identifiants des ressources ne sont pas connus à priori. Pour appliquer cette méthode, nous avons extrait des mots-clés de contenus pouvant être

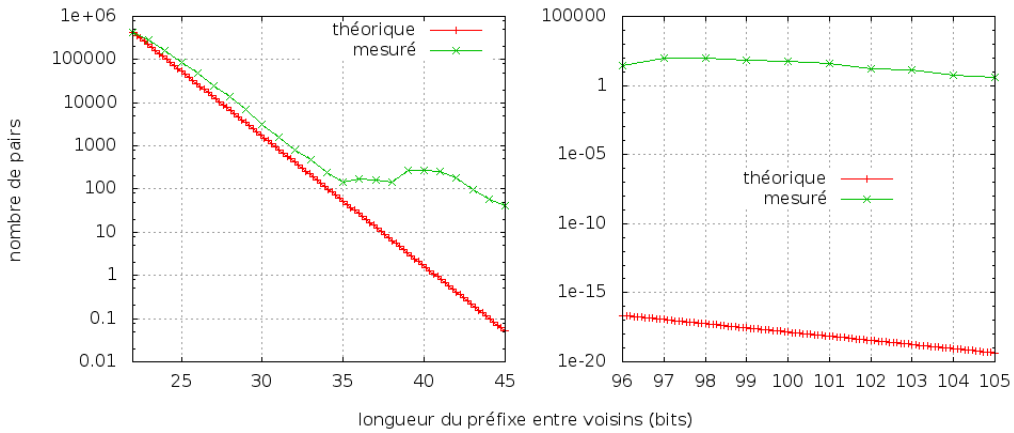

FIGURE 5. Nombre moyen de pair théorique et mesuré partageant un préfixe

partagés sur KAD depuis plusieurs sources d'information (meilleures ventes Amazon, iTunes, fichiers populaires sur ThePirateBay). Nous avons ensuite calculé l'identifiant de chacun des mots-clés composant les différents titres par la fonction MD4 utilisée par KAD. Nous avons finalement recherché les contacts étant anormalement proches de ces identifiants (partageant un préfixe supérieur à 30 bits) dans les données des explorations. Un extrait des résultats est donné ci-après.

```
[...]
twilight 4D62D26BB2A686195DA7078D3720F60A
[prefix = 122]
<4D62D26BB2A686195DA7078D3720F632,X.Y.#.#,7290,7294>
soundtrack AC213377BB53F608390BD94A6AE6DD35
[prefix = 96]
<AC213377BB53F608390BD94A82582F42,#.#.#.#,5003,5002>
harry 770CF5279AB34348C8FECF9672747B94
[prefix = 98]
<770CF5279AB34348C8FECF96524D8CDE,#.#.#.#,5003,5002>
robin B9DF47E5BFAD75F8EE5E3F50EA217983
[prefix = 96]
<B9DF47E5BFAD75F8EE5E3F5051F34AA8,#.#.#.#,5003,5002>
[prefix = 123]
<B9DF47E5BFAD75F8EE5E3F50EA21799F,X.Y.#.#,7290,7294>
[...]

216/888 of the proposed keywords are targeted with
at least96 bits by:
44 IP addresses (representing 2119 different KADID)
41 subnets /24  (representing 2155 different KADID)
```

Sur les 888 mots-clés utilisés pour cette analyse, un quart d'entre eux avait un pair proche partageant au moins 96 bits ce qui, étant donné l'espérance de trouver un pair légitime avec un tel préfixe (voir tableau I) traduit sans équivoque un placement intentionnel et un comportement malveillant. Un échantillon de ces mots-clés est donné dans le tableau II, certains faisant référence à un contenu explicite, d'autres étant plus génériques.

Pour les pairs malveillants ainsi détectés, nous avons recherché leur présence sur l'ensemble de la DHT afin de découvrir d'autres identifiants ciblés et absents de la liste initiale de mots-clés. Nous avons ainsi relevé que les seuls mots-clés recherchés ne représentent que 10% de la présence de ces clients (adresse IP + port) sur la DHT. En comptant les 216 identifiants de mots-clés initiaux, ces clients sont au total présents sur 2119 KADIDs. Ce résultat montre clairement que de nombreux contenus de la DHT sont attaqués, parmi les plus populaires. De plus, des configurations d'attaques émergent rapidement des données. Par exemple, parmi les 216 identifiants, 205 sont ciblés par des pairs ayant exactement les ports suivants : UDP=5003, TCP=5002, un préfixe de 96bits mais des adresses IP distribuées sur plusieurs réseaux. Un autre attaquant cible 16 identifiants parmi les 216 en utilisant des pairs ayant exactement les ports : UDP=7290, TCP=7294, un préfixe de 122bits et une adresse IP venant d'un sous réseau spécifique (16 de la forme `X.Y.#.#`). Même si certaines configurations utilisées par un même attaquant semblent évidentes, une caractérisation plus précise de celles-ci (adresses IP, ports, nombre de noeuds insérés, distance des noeuds, etc.) par apprentissage permettrait d'identifier plus précisément le nombre et l'importance des différents attaquants. Une étude approfondie du comportement de ces pairs par des communications directes permettrait en outre de découvrir la nature de leur activité (surveillance, pollution, DDoS, etc.).

Bien que cette estimation soit fiable, elle a également des limites, notamment quant au jeu de caractères utilisé

mot-clé	meilleur préfixe
avatar	126
invictus	123
sherlock	122
princess	122
frog	98
ncis	96
nero	96
...	...

mot-clé	meilleur préfixe
nine	122
love	122
american	97
russian	97
the	96
black	96
pirate	96
...	...

TABLE II
EXEMPLES DE MOTS-CLÉS ATTAQUÉS

par les mots-clés. Ceux considérés pour notre expérience utilisent en effet l'alphabet latin ; or, KAD est pour moitié utilisé en Asie. Les pairs ciblant spécifiquement des contenus décrits avec des caractères asiatiques peuvent échapper à cette analyse. Par ailleurs, d'autres attaques peuvent cibler exclusivement l'indéxation des fichiers et non les mots-clés, dont les identifiants peuvent être obtenus en recherchant les fichiers partagés dans KAD. Il serait tout aussi intéressant de détecter les attaques de ce point de vue.

V. Conclusion

Alors que plusieurs attaques pouvant affecter le réseau KAD ont été décrites dans de précédents travaux et que de nombreuses observations de ce réseau ont déjà été réalisées, aucune d'entre elles ne s'était intéressée jusqu'alors aux questions de sécurité affectant la DHT. Afin d'estimer les positionnements anormaux des pairs traduisant des attaques, nous avons tout d'abord développé et évalué un explorateur capable de découvrir précisément la DHT de KAD, malgré les limitations récemment incluses dans les clients.

Une première analyse considérant la proximité entre les identifiants des pairs a mis en évidence des regroupements de pairs anormaux, quelques pairs étant trop proches les uns des autres (426) mais la grande majorité d'entre eux partageant un même identifiant (248569). Une seconde analyse basée sur l'étude de mots-clés populaires a mis en évidence qu'une grande proportion de ceux-ci est attaquée. Les pairs impliqués sont d'ailleurs présents sur de nombreux identifiants de la DHT (2119) et des configurations d'attaques peuvent être clairement mises en évidence. Concernant les mots-clés ciblés, les attaquants insèrent un seul pair extrêmement proche du contenu (96 bits ou 122 bits communs) mais ne semblent en revanche pas réaliser d'attaques impliquant plusieurs pairs.

La suite de ces travaux consiste à étudier plus précisément les pairs suspects ainsi mis en évidence. Tout d'abord, en caractérisant les motifs d'attaques par des approches de fouille de données afin de mettre en évidence des similarités entre les pairs suspects, notamment dans le cadre de l'analyse par densité. Ensuite, en supervisant l'évolution de leur activité à long terme afin de détecter les nouveaux contenus ciblés. Enfin, en communiquant avec eux via les primitives du protocole KAD pour mieux identifier leur comportement (surveillance, déni de service, pollution...) et leurs moyens de mise en œuvre. Ces connaissances doivent permettre à terme le développement de nouveaux mécanismes de protection pour les futurs clients P2P.

Références

[1] M. Steiner, T. En-Najjary, and E. W. Biersack, "Exploiting kad : possible uses and misuses," *SIGCOMM Comput. Commun. Rev.*, vol. 37, no. 5, pp. 65–70, 2007.

[2] G. Memon, R. Rejaie, Y. Guo, and D. Stutzbach, "Large-scale monitoring of DHT traffic," in *International Workshop on Peer-to-Peer Systems (IPTPS)*, Boston, MA, Apr. 2009. [Online]. Available : http://www.barsoom.org/papers/iptps09-montra.pdf

[3] T. Cholez, I. Chrisment, and O. Festor, "Monitoring and Controlling Content Access in KAD," in *International Conference on Communications - ICC 2010*. Capetown Afrique Du Sud : IEEE, 05 2010. [Online]. Available : http://hal.inria.fr/inria-00490347/en/

[4] J. Liang, N. Naoumov, and K. W. Ross, "The Index Poisoning Attack in P2P File Sharing Systems," in *INFOCOM 2006. 25th IEEE International Conference on Computer Communications. Proceedings*. IEEE, 2006, pp. 1–12. [Online]. Available : http://dx.doi.org/10.1109/INFOCOM.2006.232

[5] T. Locher, D. Mysicka, S. Schmid, and R. Wattenhofer, "Poisoning the Kad Network," in *11th International Conference on Distributed Computing and Networking (ICDCN), Kolkata, India*, January 2010.

[6] N. Naoumov and K. Ross, "Exploiting p2p systems for ddos attacks," in *InfoScale '06 : Proceedings of the 1st international conference on Scalable information systems*. New York, NY, USA : ACM, 2006, p. 47.

[7] P. Wang, J. Tyra, E. Chan-Tin, T. Malchow, D. F. Kune, N. Hopper, and Y. Kim, "Attacking the kad network," in *SecureComm '08 : Proceedings of the 4th international conference on Security and privacy in communication netowrks*. New York, NY, USA : ACM, 2008, pp. 1–10.

[8] P. Maymounkov and D. Mazières, "Kademlia : A peer-to-peer information system based on the xor metric," in *IPTPS '01 : Revised Papers from the First International Workshop on Peer-to-Peer Systems*. London, UK : Springer-Verlag, 2002, pp. 53–65.

[9] J. R. Douceur, "The sybil attack," in *IPTPS '01 : Revised Papers from the First International Workshop on Peer-to-Peer Systems*. London, UK : Springer-Verlag, 2002, pp. 251–260.

[10] T. Cholez, I. Chrisment, and O. Festor, "Evaluation of Sybil Attacks Protection Schemes in KAD," in *3rd International Conference on Autonomous Infrastructure, Management and Security - AIMS 2009*, ser. Lecture Notes in Computer Science, vol. 5637, University of Twente. Enschede Pays-Bas : Springer, 2009, pp. 70–82. [Online]. Available : http://hal.inria.fr/inria-00405381/en/

[11] ——, "Efficient DHT attack mitigation through peers' ID distribution," in *Seventh International Workshop on Hot Topics in Peer-to-Peer Systems - HotP2P 2010*. Atlanta États-Unis : IEEE International Parallel & Distributed Processing Symposium, 04 2010. [Online]. Available : http://hal.inria.fr/inria-00490509/en/

[12] M. Steiner, T. En-Najjary, and E. W. Biersack, "A global view of kad," in *IMC 2007, ACM SIGCOMM Internet Measurement Conference, October 23-26, 2007, San Diego, USA*, 10 2007.

[13] J. Yu, C. Fang, J. Xu, E.-C. Chang, and Z. Li, "Id repetition in kad." in *Peer-to-Peer Computing'09*. Atlanta États-Unis : IEEE, 09 2009, pp. 111–120.